REMARKS

Claims 27-43 and 45 are currently pending in the application. On page 3 of the Office Action, claim 45 was rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 5,915,024 (Kitaori).

Kitaori is directed to an apparatus and method for adding an electronic signature to document data. According to Kitaori, the method includes dividing document data into a plurality of divided document data using as a delimiter a predetermined character appearing in a document represented by the document data, generating an electronic signature for each of the divided document data on the basis of the divided document data, and storing the divided document data, the electronic signature based on the divided document data, and information for associating the divided document data with the electronic signature. *See* Kitaori, column 4, lines 51-62.

Kitaori clearly states that only one hash function, not a first and second hash function, is applied to a signature message, which includes divided document information.

Therefore, Kitaori does not teach applying one-way *functions* to data. Moreover, Applicants respectfully submit that Kitaori fails to disclose, "appending the first and second authenticators to the data," as recited in claim 45. Further, assuming *arguendo* that Kitaori's signature is an authenticator, Kitaori clearly states that the electronic signature is added to a message. Thus, in Kitaori, only one signature is added to a message. Therefore, Kitaori does not disclose a first and second authenticator.

On page 4 of the Office Action, claims 27, 32, and 37-43 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,915,024 (Kitaori) in view of U.S. Patent No. 6,009,524 (Olarig).

Olarig discloses a system and method for FLASH BIOS upgrades. According to Olarig, each hub or node equipped with a FLASH memory is also equipped with a validation system, which ensures that a received FLASH upgrade is authorized and uncorrupted. Each set of instructions to be flashed is marked with a vendor authorization digital signature and a system administrator authorization digital signature. Before the FLASH memory will be upgraded, both digital signatures must be recognized by the validation system. Flash upgrades can be performed from any location on the network, that is, flash upgrades are not limited to an admin node, as digital signatures are used for security purposes.

Applicants respectfully submit that independent claims 27, 32, and 37-43 are patentable over Kitaori in view of Olarig, as neither Kitaori nor Olarig, alone or in combination, teaches or suggests, "applying a first one-way function" and "applying a second one-way function," as recited in claim 27, for example.

Kitaori clearly states that the digest generator applies, "a hash function" to the signature message. As is clearly illustrated in FIG. 1 of Kitaori, Kitaori applies only one hash function, for example, "MD5" or "SHA."

In the "Response to Arguments" section on page 2 of the Office Action, the Examiner alleged that Kitaori states that a signature or hash is attached to *each* piece of divided data. *See* Office Action, page 2 [emphasis added]. Applicants respectfully submit that the Examiner's allegation is false. In particular, Kitaori does not state that a signature or hash is attached to "each of a divided data."

Rather, Kitaori states that a hash function is applied to a signature message. The signature message contains divided document information. Therefore, in contrast to the present invention, in Kitaori, only one hash function is applied to the divided document information, as a group.

Moreover, Kitaori does not teach a first key and a second key, wherein the first and second keys are different as in the present invention. Kitaori indicates that only one key is used (as only one hash function is used). Further still, assuming *arugendo* that a first and second key are used as in the present invention, Kitaori provides no indication or suggestion that the keys are different.

Applicants respectfully submit that although Olarig discloses a plurality of keys, Olarig does not teach applying hash functions using keys wherein a first one of the keys is different from a second one of the keys. In Olarig, the keys are merely security keys and are used for verification of digital signatures. Thus, the keys are not used in the application of hash functions. Security keys for verification of signatures are not tantamount to keys used in the application of hash functions.

In light of the foregoing, independent claims 27, 32, and 37-43 are patentable over the references. As Herbert, Dolan, and Bellare add no relevant information to the above-identified references, the dependent claims of the present invention are patentable over the references for at least the reasons presented above for the independent claims.

If there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 9/19/06

By: _____
Reginald D. Lucas
Registration No. 46,883

1201 New York Ave, N.W., 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501